

Listing of the Claims:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

- 1 1. (Currently Amended) An electronic circuit for cryptographic processing,
2 ~~having a set of combinatorial logical circuits, the set of combinatorial logical~~
3 ~~circuits comprising:~~
4 a first combinatorial logical circuit, having an input, arranged to
5 perform a first set of logical operations on input data at the input and to
6 produce a corresponding output data, the output data having a given
7 functional relation to the input data, ~~and characterized in that the set of~~
8 ~~combinatorial logical circuits further comprises at least~~
9 a second combinatorial logical circuit, having an input, arranged to
10 perform a second set of logical operations on ~~the same~~ input data at said input
11 and to produce output data, the output data having ~~a an identical~~ functional
12 relation to the input data identical to the given functional relation,
13 wherein the first set of logical operations is different from the second set
14 of logical operations, and
15 a selector for receiving a given input data and wherein the electronic
16 ~~circuit is arranged to dynamically selecting from among the first one~~
17 ~~combinatorial logical circuit and the second combinatorial logical circuit of the~~

18 ~~set of combinatorial logical circuits~~ for performing logical operations on the
19 given the input data and producing output data, and
20 wherein the selecting includes inputting the given input data to the
21 input of the selected one of the first and second combinatorial logical
22 circuits and outputting a selected output, the selected output being the
23 output of the selected one of the first and second combinatorial logical
24 circuits.

1 2. (Currently Amended) The electronic circuit according to claim 1, further
2 comprising:

3 a third combinatorial logical circuit, having an input, arranged to
4 perform a third set of logical operations on input data at the input and to
5 produce a corresponding output data, the output data having a given
6 functional relation to the input data, and

7 a fourth combinatorial logical circuit, having an input, arranged to
8 perform a fourth set of logical operations on input data at said input and to
9 produce output data, the output data having a functional relation to the input
10 data identical to said given functional relation,

11 wherein the third set of logical operations is different from the fourth
12 set of logical operations, and

13 a selector for receiving said selected output data and dynamically
14 selecting from among the third combinatorial logical circuit and the fourth

15 combinatorial logical circuit for performing logical operations on the selected
16 output data and producing a second output data, and
17 wherein said selecting includes inputting the selected output data to the
18 input of the selected one of the third and fourth combinatorial logical circuits
19 comprising at least a first set of combinatorial logical circuits and a second
20 set of combinatorial logical circuits, and arranged to use output data
21 produced by the first set of combinatorial logical circuits as input data of
22 the second set of combinatorial logical circuits.

1 3. (Currently Amended) The ~~An~~ electronic circuit of ~~according to~~ claim 1,
2 wherein the selector comprises further comprising:
3 [[-] a selection circuit arranged for generating a signal to select one
4 combinatorial logical circuit of the set of combinatorial logical circuits,
5 [[-] a splitter circuit arranged for inputting the given input data to one of
6 the first and second combinatorial logical circuit of the set of combinatorial
7 logical circuits, depending on the signal,
8 [[-] a merger circuit arranged for outputting data from one of the first
9 and second combinatorial logical circuit of the set of combinatorial logical
10 circuits, depending on the signal.

1 4. (Currently Amended) The ~~An~~ electronic circuit of ~~according to~~ claim 3,
2 further comprising a timing circuit ~~arranged~~ to determine the points in
3 time at which the selection circuit generates the signal to select one of the

4 first and second combinatorial logical combinatorial logical circuit of the set
5 of combinatorial logical circuits.

1 5. (Currently Amended) An electronic circuit for cryptographic processing,
2 comprising:

3 [[-]] a combinatorial logical circuit ~~arranged~~ to perform logical operations on
4 input data and to produce an output data,

5 [[-]] a storage circuit element for storing the output data produced by the
6 combinatorial logical circuit, ~~characterized in that~~

7 wherein the storage electronic circuit further comprises

8 a first ~~set of an~~ encoding means for encoding the output data into a first
9 encoded output data,

10 a storage element for retrievably storing the first encoded output data,

11 a corresponding first decoding means, arranged for ~~encoding output~~
12 ~~data before storing the first output data in the storage element and decoding~~
13 the first encoded output data into said output data after retrieving the first
14 encoded output data from the storage element, ~~respectively, and~~

15 wherein the electronic circuit is arranged to dynamically control the
16 activation of the first ~~set of an~~ encoding means and the [[a]] corresponding
17 first decoding means.

1 6. (Currently Amended) The ~~An~~ electronic circuit of ~~according to~~ claim 5,
2 wherein the storage circuit further comprises comprising:

3 a second ~~set of an~~ encoding means for encoding the output data into a
4 second encoded output data for storing in the storage element.

5 a corresponding second decoding means, arranged for ~~encoding output~~
6 ~~data before storing the first output data in the storage element and decoding~~
7 ~~the second~~ encoded output data into said output data after retrieving the
8 second encoded output data from the storage element, ~~respectively,~~

9 wherein the encoding of the first output data is different from the
10 encoding of the second output data, and

11 wherein the electronic circuit is further arranged to dynamically
12 select from among the first one set of an encoding means and its [[a]]
13 corresponding first decoding means and the second ~~set of an~~ encoding
14 means and its [[a]] corresponding second decoding means, for encoding and
15 decoding of the output data.

1 7. (Currently Amended) ~~The An~~ The electronic circuit ~~of according to~~ claim 6,
2 further comprising a timing circuit ~~arranged~~ to determine the points in
3 time at which the electronic circuit selects one from among the first and
4 second set of encoding means and corresponding first and second decoding
5 means, ~~of a set comprising at least the first set of an encoding means and a~~
6 ~~corresponding decoding means and the second set of encoding means and a~~
7 ~~corresponding decoding means..~~

1 8. (Currently Amended) ~~The An~~ an electronic circuit of ~~according to~~ claim 5,
2 wherein the combinatorial logical circuit comprises;

3 a first combinatorial logical circuit, having an input, arranged to
4 perform a first set of logical operations on input data at the input and to
5 produce a corresponding output data, the output data having a given
6 functional relation to the input data, and ~~characterized in that the set of~~
7 ~~combinatorial logical circuits further comprises at least~~

8 a second combinatorial logical circuit, having an input, arranged to
9 perform a second set of logical operations on ~~the same~~ input data at said input
10 and to produce output data, the output data having a an identical functional
11 relation to the input data identical to the given functional relation,

12 wherein the first set of logical operations is different from the second set
13 of logical operations, and

14 a selector for receiving a given input data and ~~wherein the electronic~~
15 ~~circuit is arranged to dynamically selecting from among the first one~~
16 combinatorial logical circuit and the second combinatorial logical circuit of the
17 ~~set of combinatorial logical circuits for performing logical operations on the~~
18 given the input data and producing output data, and

19 wherein the selecting includes inputting the given input data to the
20 input of the selected one of the first and second combinatorial logical circuits
21 and outputting a selected output, the selected output being the output of the
22 selected one of the first and second combinatorial logical circuits.

9. (Canceled)

1 10. (Currently Amended) A method of processing cryptographic data,
2 comprising:
3 [[-]] using a set of logical operations for processing input data and producing
4 output data,
5 [[-]] storing the output data in a storage element, wherein the storing
6 ~~characterized in that the method further comprises:~~
7 [[-]] encoding the output data into an encoded output data before
8 ~~storing the output data in the storage element,~~
9 storing the encoded output data in the storage element.
10 retrieving the encoded output data from the storage element.
11 [[-]] decoding the encoded output data retrieved after retrieving from
12 the storage element, and
13 dynamically controlling the encoding of the output data into an
14 encoded output data and the corresponding decoding of the encoded
15 output data retrieved from the storage element.

1 11. (Currently Amended) A cryptographic device comprising an electronic
2 circuit according to claim 1.

1 12. (New) The electronic circuit of claim 1, wherein the selector includes:

2 a first mask circuit for selectively masking and not masking, based on
3 the signal, the given input data for input to the first combinatorial logical
4 circuit, and
5 a second mask circuit for selectively masking and not masking, based
6 on the signal, the given input data for input to the second combinatorial
7 logical circuit.

1 13. (New) The electronic circuit of claim 8, wherein the selector includes:

2 a first mask circuit to selectively mask and not mask, based on the
3 signal, the given input data and to input the selected masked and not masked
4 given input data to the first combinatorial logical circuit, and

5 a second mask circuit to selectively mask and not mask, based on the
6 signal, to input the selected masked and not masked given input data to the
7 second combinatorial logical circuit.

1 14. (New) The electronic circuit of claim 13,

2 wherein the first mask circuit includes an AND mask configured to
3 mask and to not mask the given input data by inputting to the first
4 combinatorial logical circuit a selection between all zeros and the given input
5 data, respectively and

6 wherein the second mask circuit includes an AND mask configured
7 to mask and to not mask the given input data by inputting to the second

8 combinatorial logical circuit a selection between all zeros and the given
9 input data, respectively.

1 15. (New) The electronic circuit of claim 1, wherein the selector includes an
2 OR merger circuit to receive the output of the first combinatorial logical
3 circuit and to receive the output of the second combinatorial logic circuit,
4 and to output, as the selected output, a logical OR of the output of the first
5 combinatorial logical circuit and the output of the second combinatorial
6 logic circuit.

1 16. (New) A method of processing cryptographic data, comprising:
2 generating a mode signal having one of a given plurality of states;
3 receiving a given input data and generating a cryptographic processed
4 data output, said generating including:

5 generating a first input data, wherein the first input data is a
6 selected one of a mask of the given input data and a not mask of the
7 given data, the selection based on the state of the mode signal;

8 generating a second input data, wherein the second input data is
9 the other of the mask of the given input data and the not mask of the
10 given data,

11 performing a first set of logical operations on the first input data
12 to generate a first output data, the first set of logical operations
13 embodying a given input-output function,

14 performing a second set of logical operations on the second input
15 data to generate a second output data, the second set of logical
16 operations being different than the first set of logical operations and the
17 second set of logical operations embodying the same given input-output
18 function, and
19 merging the first output data and the second output data to
20 generate the cryptographic data output;
21 repeating said generating a mode signal to have a different one of the
22 given plurality of states; and
23 repeating said receiving a given input data and generating a
24 cryptographic processed data output.